WARING'S PROBLEM FOR POLYNOMIALS IN TWO VARIABLES

ARNAUD BODIN AND MIREILLE CAR

Abstract. We prove that all polynomials in several variables can be decomposed as the sums of kth powers: $P(x_1,\ldots,x_n) = Q_1(x_1,\ldots,x_n)^k + \cdots + Q_s(x_1,\ldots,x_n)^k$, provided that elements of the base field are themselves sums of kth powers. We also give bounds for the number of terms s and the degree of the Q_i^k. We then improve these bounds in the case of two variables polynomials of large degree to get a decomposition $P(x,y) = Q_1(x,y)^k + \cdots + Q_s(x,y)^k$ with $\deg Q_i^k \leqslant \deg P + k^3$ and s that depends on k and $\ln(\deg P)$.

1. Introduction

For any domain A and any integer $k \geqslant 2$, let $W(A,k)$ denote the subset of A formed by all finite sums of kth powers a^k with $a \in A$. Let $\underline{w}_A(k)$ denote the least integer s, if it exists, such that for every element $a \in W(A,k)$, the equation

$$a = a_1^k + \cdots + a_s^k$$

admits solutions $(a_1,\ldots,a_s) \in A^s$.

The case of polynomial rings $K[t]$ over a field K is of particular interest (see [10], [7]). The similarity between the arithmetic of the ring $\mathbb{Z}$ and the arithmetic of the polynomial rings in a single variable $F[t]$ over a finite field F with q elements led to investigate a restricted variant of Waring's problem over $F[t]$, namely the strict Waring problem. For $P \in F[t]$, a representation

$$P = Q_1^k + \cdots + Q_s^k \qquad \text{with } \deg Q_i^k < \deg P + k,$$

and $Q_i \in F[t]$ is a *strict representation*.
For the strict Waring problem, analog to the classical numbers $g_{\mathbb{N}}(k)$ and $G_{\mathbb{N}}(k)$ have been defined as follows. Let $g_{F[t]}(k)$ (resp. $G_{F[t]}(k)$) denote the least integer s, if it exists, such that every polynomial in $W(F[t],k)$ (resp. every polynomial in $W(F[t],k)$ of sufficiently large degree) may be written as a sum satisfying the strict degree condition.
General results about Waring's problem for the ring of polynomials over a finite field may be found in [9], [10], [11], [12], [14] for the unrestricted

Date: January 18, 2013.
2000 *Mathematics Subject Classification.* 11P05 (13B25, 11T55).
Key words and phrases. Several variables polynomials, sum of powers, approximate roots, Vandermonde determinant.

problem and in [13], [8], [5], [3], [7] for the strict Waring problem. Gallardo's method introduced in [6] and performed in [4] to deal with Waring's problem for cubes was generalized in [3] and [7] where bounds for $g_{F[t]}(k)$ and $G_{F[t]}(k)$ were established when q and k satisfy some conditions.

The goal of this paper is a study of Waring's problem for the ring $F[x,y]$ of polynomials in two variables over a field F. As for the one variable case, two variations of Waring's problem may be considered. The first one, is the unrestricted Waring's problem; the second one takes degree conditions in account.
In Section 2 we start by some relations between Waring's problem for polynomials in one variable and Waring's problem for polynomials in $n \geqslant 2$ variables. In Section 3, we prove that, provided all elements of the field F are sums of kth powers, there exists a positive integer s (depending on F and k) such that every polynomial $P \in F[x,y]$ may be written as a sum

$$P = Q_1^k + \cdots + Q_s^k, \tag{†}$$

where for $i = 1, \dots, s$, Q_i is a polynomial of $K[x,y]$ such that $\deg Q_i \leqslant \deg P$. We then prove various improvements, the goal being to have in representations (†) a decomposition with the following properties: the first priority is to have the lowest possible degree for the polynomials Q_i and the second priority is a small number of terms. In Section 5, we prove that (†) is possible for polynomials of large degree with $\deg Q_i^k \leqslant \deg P + k^3$, the number s of terms depending on F, k and $\deg P$. To do that, in Section 4, we introduce the notion of approximate root.

Let F be a field such that: F has more than k elements, the characteristic of F does not divide k and each element of F can be written as a sum of $w_F(k)$ kth powers of elements of F. We summarize in the tabular below the different bounds we get for a decomposition of a polynomial $P(x,y)$ of degree d as a sum $P = \sum_{i=1}^s Q_i^k$.

	$\deg Q_i^k$	s
Corollary 4	kd	$kw_F(k)$
Proposition 5	$d + 2(k-1)^2$	$\frac{1}{2}k(d+1)(d+2)w_F(k)$
Proposition 6	$2d + 4k^2$	$k^2(2k-1)w_F(k)$
Theorem 8	$d + k^3$	$2k^3 \ln(\frac{d}{k}+1)\ln(2k) + 7k^4\ln(k)w_F(k)^2$

The two basic results are Corollary 4 that give a decomposition with very few terms of high degree and Proposition 5 with many terms of low degree. Our first main result is Proposition 6, that provides a decomposition with terms of medium degree, but the number of terms depends only on k and not on the degree of P. Then Theorem 8 decomposes P, of sufficiently large degree $d \geqslant 2k^4$, into a sum of few terms of low degree.

For instance, let a field with $w_F(k) = 1$ (that is to say each element of F is a kth power), set $d = 200$ and $k = 3$, then each polynomial $P(x, y)$ of degree 200 can be written $P = \sum_{i=1}^{s} Q_i^3$ with[1]

	$\deg Q_i^k$	s
Corollary 4	600	3
Proposition 5	208	60903
Proposition 6	436	45
Theorem 8	227	812

2. The unrestricted Waring's problem

If A is a domain, we denote by $W(A, k, s)$ the set of elements $a \in A$ that can be written as a sum $a = a_1^k + \cdots + a_s^k$ with $a_1, \ldots, a_s \in A$; if $A = W(A, k, s)$ for an integer s, then for any integer $s' \geqslant s$, we have $A = W(A, k, s')$. Let $w_A(k)$ denote the least integer s such that $A = W(A, k, s)$. If such a s does not exist, let $w_A(k) = \infty$. Observe that $w_A(k) \geqslant \underline{w}_A(k)$ and in the case that $A = W(A, k)$ then $w_A(k) = \underline{w}_A(k)$. In this section we are concerned with rings of polynomials in $n \geqslant 1$ variables.

Lemma 1. *Let A be a domain and let s be a positive integer.*

(1) *If $A[t] = W(A[t], k, s)$, then $A = W(A, k, s)$, so that $w_A(k) \leqslant w_{A[t]}(k)$.*
(2) *$A[t] = W(A[t], k, s)$ if and only if $A[x_1, \ldots, x_n] = W(A[x_1, \ldots, x_n], k, s)$, so that $w_{A[x_1,\ldots,x_n]}(k) = w_{A[t]}(k)$.*

A kind of reciprocal to (1) will be discussed later in Proposition 3.
Proof

(1) Suppose $A[t] = W(A[t], k, s)$. Every $a \in A$ is a sum $a = Q_1^k + \cdots + Q_s^k$ for some $Q_i \in A[t]$. Specializing t at 1 for instance, gives $a = Q_1(1)^k + \cdots + Q_s(1)^k$, a sum in A. Therefore, $w_{A[t]}(k) \geqslant w_A(k)$.
(2) (a) If $A[t] = W(A[t], k, s)$, then there exist $Q_1, \ldots, Q_s \in A[t]$ such that $t = Q_1(t)^k + \cdots + Q_s(t)^k$. Pick $P \in A[x_1, \ldots, x_n]$ and substitute P for t, we get: $P(x_1, \ldots, x_n) = Q_1(P(x_1, \ldots, x_n))^k + \cdots + Q_s(P(x_1, \ldots, x_n))^k$. Hence $w_{A[x_1,\ldots,x_n]}(k) \leqslant w_{A[t]}(k)$.
    (b) If $A[x_1, \ldots, x_n] = W(A[x_1, \ldots, x_n], k, s)$ then any $P(t) \in A[t]$ can be written $P(t) = Q_1(t, x_2, \ldots, x_n)^k + \cdots + Q_s(t, x_2, \ldots, x_n)^k$. By the specialization $x_2 = \cdots = x_n = 1$ we get that $P(t) \in W(A[t], k, s)$. Therefore $w_{A[x_1,\ldots,x_n]}(k) \geqslant w_{A[t]}(k)$.

Remark. It is also true that $A[t] = W(A[t], k, s)$ if and only if $t \in W(A[t], k, s)$.

This remark motivates the fact that we consider Waring's problem for a polynomial ring $F[x_1, \ldots, x_n]$ where F is a field satisfying the condition

[1] In fact the last bound comes from a sharper bound obtained in the proof of Theorem 8.

$F = W(F,k)$. Such a field is called a *Waring field for the exponent* k, or briefly, a k-*Waring field*.
Let us give some examples. An algebraically closed field F is a k-Waring field with $w_F(k) = 1$ for every positive integer k. If F is a finite field of characteristic p, for every positive integer n, F is a p^n-Waring field with $w_F(p^n) = 1$. It is known, c.f. [1], [5], that for a finite field F of characteristic p that does not divide k and order $q = p^m$, F is a Waring field for the exponent k if and only if for all $d \neq m$ dividing m, $(q-1)/(p^d-1)$ does not divide k.
When F has prime characteristic p, it is sufficient to consider Waring's problem for exponents k coprime with p. Indeed, we have

Proposition 2. *Let $k \geqslant 2$ be coprime with p. Then, for any positive integer ν and for any positive integer s, we have*

$$W(F[x_1,\ldots,x_n], kp^\nu, s) = \left\{ Q^{p^\nu} \mid Q \in W(F[x_1,\ldots,x_n],k,s)) \right\},$$

$$w_{F[x_1,\ldots,x_n]}(kp^\nu) = w_{F[x_1,\ldots,x_n]}(k).$$

The proof is similar to that of [3, Theorem 2.1] and relies on the relation $(Q_1^k + \cdots + Q_s^k)^p = Q_1^{pk} + \cdots + Q_s^{pk}$.

3. Vandermonde determinants

3.1. **Sum with high degree.** Let us recall that for $(\alpha_1,\ldots,\alpha_n) \in L^n$, where L is a field containing F, Vandermonde's determinant $V(\alpha_1,\ldots,\alpha_n)$ verifies:

$$V(\alpha_1,\ldots,\alpha_n) := \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j). \tag{1}$$

Proposition 3. *Let F be a field with more than k elements, whose characteristic does not divide k, such that each element of F can be written as a sum of kth powers of elements of F. Then any polynomial $P(x_1,\ldots,x_n)$ with coefficients in the field F is a sum of kth powers. In other words, for any positive integer n,*

$$F[x_1,\ldots,x_n] = W(F[x_1,\ldots,x_n],k).$$

Proof. The proof follows ideas from [7]. Let $\alpha_1,\ldots,\alpha_k$ be distinct elements of F. First notice that by formula (1), if t is any transcendental element over F, $V(\alpha_1,\ldots,\alpha_k) = V(t+\alpha_1,\ldots,t+\alpha_k)$. By expanding the determinant $V(t+\alpha_1,\ldots,t+\alpha_k)$ along the last column we get (a term marked $\check{x}_i$ means

that it is omitted):

$$\begin{aligned}V(\alpha_1,\ldots,\alpha_k) &= V(t+\alpha_1,\ldots,t+\alpha_k)\\ &= \pm\sum_{i=1}^{k}(-1)^i(t+\alpha_i)^{k-1}V(t+\alpha_1,\ldots,\overbrace{t+\alpha_i}^{\vee},\ldots,t+\alpha_k)\\ &= \pm\sum_{i=1}^{k}(-1)^i(t+\alpha_i)^{k-1}V(\alpha_1,\ldots,\check{\alpha}_i,\ldots,\alpha_k).\end{aligned}$$

The constant $\gamma = V(\alpha_1,\ldots,\alpha_k)$ is non-zero since the α_i are distinct elements of F. We write

$$\sum_{i=1}^{k}\frac{(t+\alpha_i)^{k-1}}{\beta_i} = \gamma,$$

where β_i are non-zero constants in F. This formula proves that the function $C(t) = \sum_{i=1}^{k}\frac{(t+\alpha_i)^k}{\beta_i} - \gamma kt$ has an identically null derivative; since the characteristic of F does not divide k, it implies that $C(t)$ is a constant. So that, for some $\delta \in F$:

$$\sum_{i=1}^{k}\frac{(t+\alpha_i)^k}{\beta_i} = \gamma kt + \delta. \tag{2}$$

Let $P(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$. By substitution of t by $(P-\delta)/(\gamma k)$ in equality (2) we get $P = \sum_{i=1}^{k}\frac{(P-\delta+\alpha_i\gamma k)^k}{\beta_i(\gamma k)^k}$. But by assumption $1/\beta_i(\gamma k)^k$ is a sum of kth powers of elements of F. So that $P(x_1,\ldots,x_n)$ is also a sum of kth powers of elements of $F[x_1,\ldots,x_n]$. □

Corollary 4. *Let F have more than k distinct elements such that its characteristic does not divide k. Every polynomial $P(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ of degree d can be written as a sum*

$$P(x_1,\ldots,x_n) = \delta_1 Q_1(x_1,\ldots,x_n)^k + \cdots + \delta_k Q_k(x_1,\ldots,x_n)^k,$$

where $\delta_1,\ldots,\delta_k \in F$ and $Q_1,\ldots,Q_k$ are polynomials in $F[x_1,\ldots,x_n]$ such that $\deg Q_i^k \leqslant kd$. If moreover each element of F is a sum of $w_F(k)$ kth powers, then

$$P(x_1,\ldots,x_n) = Q_1(x_1,\ldots,x_n)^k + \cdots + Q_s(x_1,\ldots,x_n)^k$$

where $Q_1,\ldots,Q_s \in F[x_1,\ldots,x_n]$ such that $\deg {Q_i}^k \leqslant kd$ for some $s \leqslant k \cdot w_F(k)$.

Proof. It comes from formula (2) and the discussion below it. □

In the sequel, we consider polynomials in two variables.

3.2. **Low degree, many terms.**

Proposition 5. *Let F be a field with more than k distinct elements such that its characteristic does not divide k. Every polynomial $P \in F[x,y]$ of degree d admits a decomposition:*

$$P(x,y) = \delta_1 Q_1(x,y)^k + \cdots + \delta_s Q_s(x,y)^k,$$

where $\delta_1, \ldots, \delta_s \in F$ and $Q_1, \ldots, Q_s$ are polynomials in $F[x,y]$ such that $\deg Q_i^k \leqslant d + 2(k-1)^2$ and $s \leqslant k \cdot \frac{(d+1)(d+2)}{2}$.
If moreover each element of F is a sum of kth powers then P admits a decomposition:

$$P(x,y) = Q_1(x,y)^k + \cdots + Q_s(x,y)^k,$$

where $Q_1, \ldots, Q_s \in F[x,y]$ with $\deg Q_i^k \leqslant d+2(k-1)^2$ and $s \leqslant kw_F(k)\frac{(d+1)(d+2)}{2}$.

Proof. Let $P(x,y) = \sum a_{i,j} x^i y^j$. We make the Euclidean divisions: $i = pk + a$ and $j = qk + b$ with $0 \leqslant a, b < k$. Each monomial $x^i y^j$ can now be written $x^i y^j = (x^p y^q)^k \cdot x^a y^b$. By Corollary 4, $x^a y^b$ can be written $x^a y^b = \delta_1 Q_1(x,y)^k + \cdots + \delta_k Q_k(x,y)^k$ with $\delta_1, \ldots, \delta_k \in F$, $Q_1, \ldots, Q_k \in F[x,y]$ and $\deg Q_i \leqslant \deg(x^a y^b)$, so that

$$x^i y^j = \delta_1 (x^p y^q Q_1(x,y))^k + \cdots + \delta_k (x^p y^q Q_1(x,y))^k.$$

Moreover $\deg((x^p y^q Q_i(x,y))^k) = k(p + q + \deg Q_i) \leqslant kp + kq + ka + kb = i + j + (k-1)(a+b) \leqslant i + j + 2(k-1)^2 \leqslant d + 2(k-1)^2$.
As $\deg P = d$ the number of monomials $x^i y^j$ is less or equal than $\frac{(d+1)(d+2)}{2}$, so that P admits a decomposition $P(x,y) = \delta_1 Q_1(x,y)^k + \cdots + \delta_s Q_s(x,y)^k$ with $\deg Q_i^k \leqslant d + 2(k-1)^2$ and $s \leqslant k\frac{(d+1)(d+2)}{2}$. Thus we can find a decomposition $P(x,y) = Q_1(x,y)^k + \cdots + Q_s(x,y)^k$ for some $s \leqslant kw_F(k)\frac{(d+1)(d+2)}{2}$. □

3.3. **Medium degree, few terms.** We improve this method to get fewer terms in the sum but the degree of each term is higher.

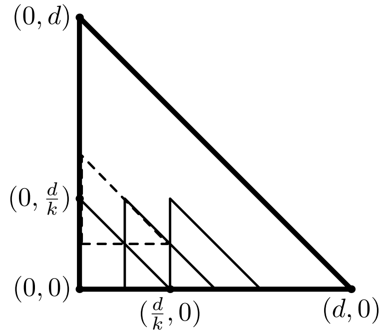
Proposition 6. *Let F be a field with more than k elements, such that its characteristic does not divide k and each element of F is a sum of kth powers. Any $P \in F[x,y]$ P admits a decomposition:*

$$P(x,y) = Q_1(x,y)^k + \cdots + Q_s(x,y)^k,$$

where $Q_1, \ldots, Q_s$ are polynomials in $F[x,y]$ with $\deg Q_i^k \leqslant 2 \deg P + 4k^2$ and $s \leqslant k^2(2k-1)w_F(k)$.

Observe that the bound for s does not depend on the degree of the polynomial P.
Proof.

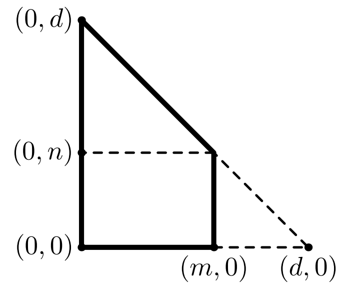
Let d be the least multiple of $2k^2$ such that $d \geqslant \deg P$. The Newton polygon of P is included in the triangle ABC with $A(0,0)$, $B(0,d)$, $C(d,0)$.



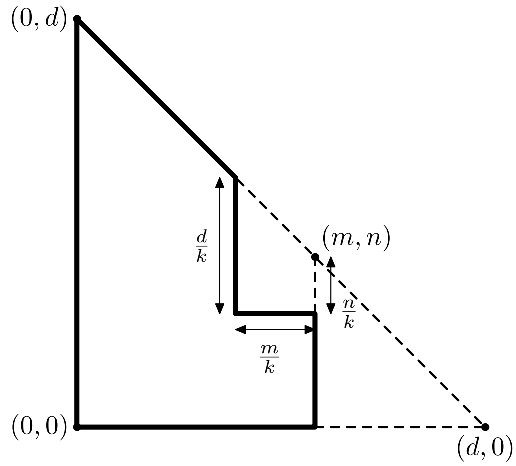
We cover this triangle ABC by $k(2k-1)$ small triangles that are translations (by $\frac{d}{2k}$-units) of $A'B'C'$ with $A'(0,0)$, $B'(0,\frac{d}{k})$, $C'(\frac{d}{k},0)$. This covering means that we can write $P(x,y)$ as a sum of $k(2k-1)$ polynomials of the form $x^{i\frac{d}{2k}}y^{j\frac{d}{2k}}P_{i,j}(x,y)$ with $\deg P_{i,j} \leqslant \frac{d}{k}$ and $0 \leqslant i+j \leqslant 2k-2$ (so that $\deg x^{i\frac{d}{2k}}y^{j\frac{d}{2k}} < d$). As $2k^2$ divides d then $x^{i\frac{d}{2k}}y^{j\frac{d}{2k}}$ is a kth power. Furthermore, by Corollary 4, we can write each $P_{i,j}$ as a sum of $kw_F(k)$ powers, each power being of degree at most $k\frac{d}{k} = d$. Hence we get a decomposition $P(x,y) = Q_1(x,y)^k + \cdots + Q_s(x,y)^k$ with $s \leqslant k^2(2k-1)w_F(k)$ terms and $\deg Q_i^k < 2d$. $\square$

4. Approximate root

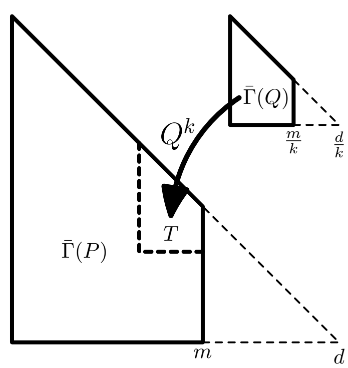
In this section F is a field whose characteristic does not divide k. Let $P \in F[x,y]$ be a polynomial that verifies the following conditions: $\deg P \leqslant d$, $\deg_x P < m$. So that the Newton polygon $\Gamma(P)$ of P is (included in) the following polygon $\bar{\Gamma}(P)$ (whose vertices are $(0,0)$, $(m,0)$, (m,n), $(0,d)$). We set $n = d-m$ and we suppose that $k|m, \quad k|n, \quad k|d$. We will look for a $Q \in F[x,y]$ such that $\deg Q \leqslant \frac{d}{k}, \deg_x Q \leqslant \frac{m}{k}$, so that $\Gamma(Q^k) \subset \bar{\Gamma}(P)$. In fact the Newton polygon of Q is homothetic to the one of P with a ratio $\frac{1}{k}$.



Proposition 7. *There exists a unique $Q(x,y) \in F[x,y]$, monic in x, such that $P + x^m y^n - Q^k$ has no monomial x^iy^j with $i \geqslant m - \frac{m}{k}$ and $j \geqslant n - \frac{n}{k}$. That is to say, the Newton polygon of $P + x^m y^n - Q^k$ is (included in):*



It means that with two kth powers ($x^m y^n$ and Q^k) we "cancel" the trapezium T (defined by the vertices (m,n), $(m, n-\frac{n}{k})$, $(m-\frac{m}{k}, n-\frac{n}{k})$,$(m-\frac{m}{k}, n+\frac{d}{k}-\frac{n}{k})$). This procedure is similar to the computation of the approximate kth root of a one variable polynomial, see [2]. The proof is sketched into the following picture:



Morally, the coefficients of Q provide a set of unknowns, which is chosen in order that Q^k and P can be identified into the trapezium area (T).

Proof. We write P as the sum $P = P_1 + P_2$ corresponding to the decomposition into two areas of $\bar{\Gamma}(P) = T \cup (\bar{\Gamma}(P) \setminus T)$: we write P_1 as a polynomial in x whose coefficients are in $F[y]$ so that $P_1(x,y) = a_1(y)x^{m-1} + \cdots + a_{\frac{m}{k}}(y)x^{m-\frac{m}{k}}$ with $\deg a_i(y) \leqslant n+i$ and $\operatorname{val} a_i(y) \geqslant n - \frac{n}{k}$. We denote by val the y-adic valuation: $\operatorname{val} \sum \alpha_i y^i = \min\{i \mid \alpha_i \neq 0\}$.

We set $P_1'(x,y) = y^n x^m + P_1(x,y)$ and $a_0(y) = y^n$. Notice that we have added a kth power since $k|m$ and $k|n$.

We also write $Q(x,y)$ as a polynomial in x with coefficients in $F[y]$: $Q(x,y) = b_0(y)x^{\frac{m}{k}} + b_1(y)x^{\frac{m}{k}-1} + \cdots + b_{\frac{m}{k}}(y)$.

We now identify the monomials of $P_1'(x,y) = x^m y^n + P_1(x,y)$ with the monomials of $Q(x,y)^k$, in the trapezium T. As we only want to identify the monomials of a sufficiently high degree we define the following equivalence:

$$a(y) \doteq b(y) \quad \text{if and only if} \quad \deg(a(y) - b(y)) < n - \frac{n}{k}.$$

It yields the following polynomial system of equations ($a_i(y)$ are data, and $b_i(y)$ unknowns):

$$(\mathcal{S}) \qquad \begin{cases} a_0 \doteq b_0^k \\ a_1 \doteq k b_0^{k-1} b_1 \\ a_2 \doteq k b_0^{k-1} b_2 + \binom{k}{2} b_0^{k-2} b_1^2 \\ \vdots \\ a_\ell \doteq k b_0^{k-1} b_\ell + \displaystyle\sum_{\substack{i_1 + 2i_2 + \cdots + (\ell-1) i_{\ell-1} = \ell \\ i_0 + i_1 + i_2 + \cdots + i_{\ell-1} = k}} c_{i_1 \ldots i_{\ell-1}} b_0^{i_0} b_1^{i_1} \cdots b_{\ell-1}^{i_{\ell-1}}, \qquad 1 \leqslant \ell \leqslant \frac{m}{k}, \end{cases}$$

where the coefficients $c_{i_1 \ldots i_{\ell-1}}$ are the multinomial coefficients defined by the following formula:

$$c_{i_1 \ldots i_{\ell-1}} = \binom{k}{i_1, \ldots, i_{\ell-1}} = \frac{k!}{i_1! \cdots i_{\ell-1}! (k - i_1 - \cdots - i_{\ell-1})!}.$$

The first equation has a solution $b_0(y) = y^{\frac{n}{k}}$. Then, as $\operatorname{val} a_1(y) \geqslant n - \frac{n}{k}$, we have $b_1(y) = \frac{1}{k} \frac{a_1(y)}{b_0(y)^{k-1}} \in F[y]$ (k is invertible in F). Next we compute $b_2(y)$,... by induction using the fact that system $(\mathcal{S})$ is triangular. Suppose that $b_0(y), b_1(y), \ldots, b_{\ell-1}(y)$ have been found. System $(\mathcal{S})$ provides the relation:

$$a_\ell \doteq k b_0^{k-1} b_\ell + \sum c_{i_1 \ldots i_{\ell-1}} b_0^{i_0} b_1^{i_1} \cdots b_{\ell-1}^{i_{\ell-1}}.$$

As $b_0(y) = y^{\frac{n}{k}}$ it means that the polynomials $k y^{n - \frac{n}{k}} b_\ell(y)$ and $a_\ell - \sum c_{i_1 \ldots i_{\ell-1}} b_0^{i_0} b_1^{i_1} \cdots b_{\ell-1}^{i_{\ell-1}}$ have equal coefficients associated to monomials y^i with $i \geqslant n - \frac{n}{k}$. Whence $b_\ell(y)$ is uniquely determined. We have proved that system $(\mathcal{S})$ has a unique solution $(b_0(y), b_1(y), \ldots, b_{\frac{m}{k}}(y))$.

Finally, we need to prove that $\deg b_i \leqslant \frac{n}{k} + i$ for $0 \leqslant i \leqslant \frac{m}{k}$. We have $b_0(y) = y^{\frac{n}{k}}$, so that $\deg b_0 = \frac{n}{k}$ and $b_1(y) = \frac{1}{k} \frac{a_1(y)}{\left(y^{\frac{n}{k}}\right)^{k-1}}$; thus, $\deg b_1 \leqslant \deg a_1 - n + \frac{n}{k} \leqslant n + 1 - n + \frac{n}{k} = \frac{n}{k} + 1$. Then, by induction we get

$$\begin{aligned} \deg b_0^{i_0} b_1^{i_1} \cdots b_{\ell-1}^{i_{\ell-1}} &\leqslant i_0 \left(\frac{n}{k} + 0\right) + i_1 \left(\frac{n}{k} + 1\right) + \cdots + i_\ell \left(\frac{n}{k} + \ell\right) \\ &= \frac{n}{k}(i_0 + i_1 + \cdots + i_\ell) + i_1 + 2i_2 + \cdots + (\ell-1) i_{\ell-1} \\ &= \frac{n}{k} k + \ell \\ &= n + \ell. \end{aligned}$$

We also find $\deg a_\ell \leqslant n + \ell$ so that $\deg b_\ell \leqslant \frac{n}{k} + \ell$. $\square$

5. Strict sum of kth powers

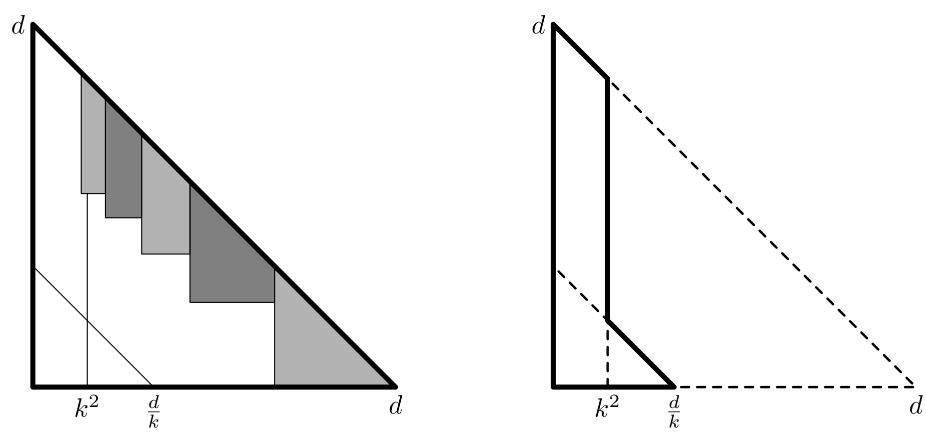
This section is devoted to the proof of the main theorem:

Theorem 8. *Let F be a field with more than k elements, whose characteristic does not divide k, such that each element of F can be written as a sum of $w_F(k)$ kth powers of elements of F. Each polynomial $P(x, y) \in F[x, y]$ of degree $d \geqslant 2k^4$ is the sum of kth powers*

$$P(x, y) = Q_1(x, y)^k + \cdots + Q_s(x, y)^k,$$

of polynomials $Q_i \in F[x, y]$ with $\deg Q_i^k \leqslant d + k^3$ and $s \leqslant 2k^3 \ln(\frac{d}{k} + 1)\ln(2k) + 7k^4 \ln(k) w_F(k)^2$.

The bound for s is derived from a sharper bound given at the end of the proof. We start by sketching the proof by pictures:

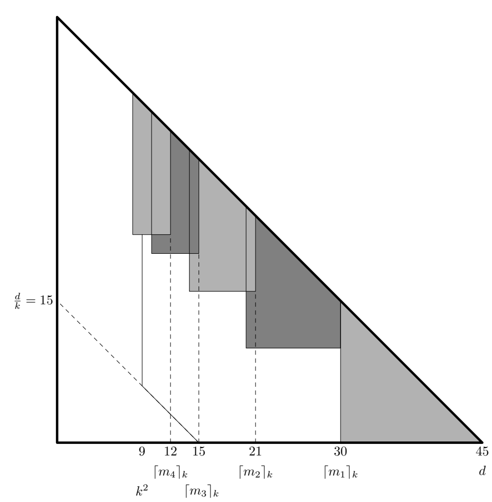


We consider the Newton polygon of P, it is included in a large triangle (see the left figure). We first cut off trapeziums, corresponding to monomials of higher degree. Each trapezium corresponds to a polynomial Q_i^k computed by an approximate kth root as explained in Section 4. It enables to lower the degree of P, except for monomials whose degree in x is less than k^2 that will be treated at the end. We iterate this process until we get a polynomial of degree less than $\frac{d}{k}$ (right figure) to which we will apply Corollary 4.

Notation. We will denote $\lceil x \rceil_k = k \left\lceil \frac{x}{k} \right\rceil$ the least integer larger or equal to x and divisible by k.

First step: lower the degree. Set $d = \deg P$, $m_0 = \lceil d \rceil_k$ and $P_0 := P$. We apply Proposition 7 to $P_0 = P$, with P_0 considered as a polynomial of total degree $\leqslant m_0$ and $m = m_0$, $n = 0$. It yields a polynomial $Q_0(x, y)$ such that $\deg_x(P + x^{m_0} - Q_0^k) < m_0 - \frac{m_0}{k}$. That is to say we have canceled a trapezium, which is there the triangle $(m_0, 0)$, $(m_0 - \frac{m_0}{k}, 0)$, $(m_0 - \frac{m_0}{k}, \frac{m_0}{k})$.

We then set $m_1 = \lceil m_0 \rceil_k - \frac{\lceil m_0 \rceil_k}{k}$ and $P_1 = P_0 + x^{m_0} - Q_0^k$. Note that $\deg_x P_1 < m_1$ and we apply Proposition 7 to P_1.
To iterate the process, consider the decomposition $P_i = P_i' + x^{m_i} \cdot P_i''$ with $\deg_x P_i' < m_i$. We apply Proposition 7 to P_i' (with $m = \lceil m_i \rceil_k$ and $n = n_i$ such that $\lceil m_i \rceil_k + n_i = m_0$) that yields Q_i such that $P_i' + x^{\lceil m_i \rceil_k} y^{n_i} - Q_i^k$ has no monomials in the corresponding trapezium whose x-coordinates are in between $\lceil m_i \rceil_k$ and $m_{i+1} := \lceil m_i \rceil_k - \frac{\lceil m_i \rceil_k}{k}$. Notice that $P_{i+1} := P_i' + x^{\lceil m_i \rceil_k} y^{n_i} - Q_i^k + x^{m_i} \cdot P_i''$ also does not have monomials in this trapezium.
Here is an example, set $d = 45$ and $k = 3$ then we get $m_0 = 45$, $m_1 = 30$, $m_2 = 20$, $m_3 = 14$, $m_4 = 10$, $m_5 = 8$ and then we stop since $m_5 < k^2$. It implies that the first trapezium has its x-coordinates in between 45 and 30, the second one between 30 and 20,... The height of the left side of each trapezium is always $\frac{d}{k} = 15$. The picture is the following:



End of iterations. We iterate the process until we reach monomials whose degree in x is less than k^2. That is to say we look for ℓ such that $m_\ell \leqslant k^2$. First notice that

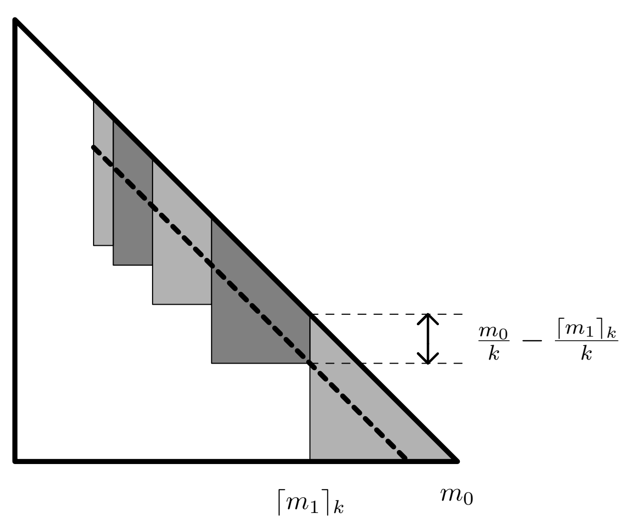
$$\begin{aligned} m_{i+1} &= \lceil m_i \rceil_k - \frac{\lceil m_i \rceil_k}{k} \\ &= (k-1) \left\lceil \frac{m_i}{k} \right\rceil \\ &\leqslant \left(1 - \frac{1}{k}\right) m_i + k - 1. \end{aligned}$$

Then, by induction

$$\begin{aligned}
m_i &\leqslant \left(1-\frac{1}{k}\right)^i m_0 + (k-1)\left(1+\left(1-\frac{1}{k}\right)+\left(1-\frac{1}{k}\right)^2+\cdots+\left(1-\frac{1}{k}\right)^{i-1}\right)\\
&\leqslant \left(1-\frac{1}{k}\right)^i m_0 + k(k-1)\\
&\leqslant (d+k)e^{-\frac{i}{k}} + k(k-1), \qquad \text{since } \left(1-\frac{1}{k}\right) \leqslant e^{-\frac{1}{k}}.
\end{aligned}$$

Now, for $\ell \geqslant k\ln(\frac{d}{k}+1)$ we get $m_\ell \leqslant k^2$.

Fall of the total degree. At the end of the first series of iterations the total degree (of the monomials whose degree in x is more or equal to k^2) falls (see the picture below).



We give a lower bound for this fall δ_0 of the degree (starting from degree m_0):

$$\begin{aligned}
\delta_0 &\geqslant \frac{m_0}{k} - \frac{\lceil m_1 \rceil_k}{k} \\
&= \left\lceil \frac{d}{k} \right\rceil - \left\lceil \frac{k\left\lceil \frac{d}{k} \right\rceil - \left\lceil \frac{d}{k} \right\rceil}{k} \right\rceil \quad (\text{since } d = \lceil m_0 \rceil_k) \\
&\geqslant \left\lfloor \frac{\left\lceil \frac{d}{k} \right\rceil}{k} \right\rfloor \\
&\geqslant \frac{d}{k^2} - 1.
\end{aligned}$$

Therefore the total degree, starting now from degree d, of the monomials whose degree in x is more than k^2 has fallen of more that $\delta \geqslant \frac{d}{k^2} - k$.

Iteration of the fall. Set $d_0 = d$. At each series of iterations the degree (of the monomials whose degree in x is more or equal to k^2) falls from d_i to $d_{i+1} := d_i - \left\lfloor \frac{d_i}{k^2} - k \right\rfloor \leqslant \left(1 - \frac{1}{k^2}\right) d_i + k$, so that (by a computation similar to the one for m_i above) $d_i \leqslant de^{-\frac{i}{k^2}} + k^3$. Suppose that $d \geqslant 2k^4$, so that $\frac{d}{2k} + k^3 \leqslant \frac{d}{k}$. Then for $\ell \geqslant k^2 \ln(2k)$, we get $d_\ell \leqslant \frac{d}{k}$. Each fall of the degree needs less than $k \ln(\frac{d}{k} + 1)$ iterations, so that we need to apply Proposition 7 many times, to get a total of $s_0 = 2k \ln(\frac{d}{k} + 1) \times k^2 \ln(2k)$ kth powers.

Monomials of low degree in x. At this point, we have written $P = \sum_{i=1}^{s_0} Q_i^k + P_1 + P_2$, where $Q_1, \ldots, Q_{s_0}, P_1, P_2 \in F[x,y]$ are such that $\deg Q_i^k \leqslant \lceil d \rceil_k$, $\deg_x P_1 < k^2$, $\deg P_2 \leqslant \frac{d}{k}$ (see the right picture below Theorem 8). By Corollary 4 we can write P_2 as a sum $P_2 = \sum_{i=1}^{s_2} Q_{i,2}^k$ of $s_2 \leqslant k w_F(k)$ terms and $\deg Q_{i,2}^k \leqslant k \left\lceil \frac{d}{k} \right\rceil = \lceil d \rceil_k < d + k$.
Now write $P_1(x,y) = \sum_{0 \leqslant j < k^2} x^j R_j(y)$, where $R_j \in F[y]$ with $\deg R_j \leqslant d - j$. By Corollary 4, write each x^j as the sum of $k w_F(k)$ terms of degree $\leqslant jk$. Then, for each $R_j(y)$ we apply the result in one variable [7, Theorem 1.4 (iii)] (or we can do a similar work as before) so that we can write (since $d \geqslant 2k^4$): $R_j(y) = \sum_{i=1}^{s} S_{ij}^k(y)$ with $s \leqslant k(w_F(k) + 3\ln(k)) + 2$ and $\deg S_{ij}^k \leqslant \deg R_j + k - 1$. We get $x^j R_j(y)$ as the sum of $s' \leqslant k w_F(k)(k(w_F(k) + 3\ln(k)) + 2)$, kth powers of degree $\leqslant jk + \deg R_j + k - 1 \leqslant d + k^3$ $(j = 0, \ldots, k^2 - 1)$. Therefore, $P_1 = \sum_{i=1}^{s_1} Q_{i,1}^k$ with $s_1 \leqslant k^3 w_F(k)(k(w_F(k) + 3\ln(k)) + 2)$ terms and $\deg Q_{i,1}^k \leqslant d + k^3$.

Conclusion. For $d \geqslant 2k^4$ we can write $P(x,y)$ as the sum

$$P(x,y) = \sum_{i=1}^{s} Q_i^k(x,y)$$

such that $\deg Q_i^k \leqslant d + k^3$ and $s \leqslant s_0 + s_2 + s_1$ that is to say[2]

$$s \leqslant 2k^3 \ln\left(\frac{d}{k} + 1\right) \ln(2k) + kw_F(k) + k^3 w_F(k)(k(w_F(k) + 3\ln(k)) + 2).$$

It yields the announced bound $s \leqslant 2k^3 \ln(\frac{d}{k} + 1)\ln(2k) + 7k^4 \ln(k) w_F(k)^2$.

Question. Is it possible to have a sum

$$P(x, y) = \sum_{i=1}^{s} Q_i^k(x, y)$$

such that $\deg Q_i^k \leqslant \deg P + k^3$ and a bound s depending only on k and not on $\deg P$?

References

[1] M. Bhaskaran, *Sums of mth powers in algebraic and abelian number fields.* Arch. Math. (Basel) 17 (1966), 497-504; Correction, ibid. 22 (1971), 370-371.

[2] A. Bodin, *Decomposition of polynomials and approximate roots.* Proc. Amer. Math. Soc. 138 (2010), 1989-1994.

[3] M. Car, *New bounds on some parameters in the Waring problem for polynomials over a finite field.* Contemporary Mathematics 461 (2008), 59-77.

[4] M. Car, L. Gallardo, *Sums of cubes of polynomials.* Acta Arith. 112 (2004), 41-50.

[5] G. Effinger, D. Hayes, *Additive number theory of polynomials over a finite field.* Oxford Mathematical Monographs, Clarendon Press, Oxford (1991).

[6] L. H. Gallardo, *On the restricted Waring problem over $\mathbf{F}_{2^n}[t]$.* Acta Arith. 42 (2000), 109-113.

[7] L. Gallardo, L. Vaserstein, *The strict Waring problem for polynomial rings.* J. Number Theory 128 (2008), 2963–2972.

[8] R.M. Kubota, *Waring's problem for $\mathbf{F}_q[x]$.* Dissertationes Math. (Rozprawy Mat.) 117 (1974).

[9] R.E.A.C Paley, *Theorems on polynomials in a Galois field.* Quarterly J. of Math. 4 (1933), 52-63.

[10] L.N. Vaserstein, *Waring's problem for algebras over fields.* J. Number Theory 26 (1987), 286-298.

[11] L.N. Vaserstein, *Sums of cubes in polynomial rings.* Math. Comput. 193 (1991), 349-357.

[12] L.N. Vaserstein, *Ramsey's theorem and Waring's problem.* In *The Arithmetic of Function Fields* (eds D. Goss and al), de Gruyter, NewYork-Berlin, (1992).

[13] W.A. Webb, *Waring's problem in $GF[q, x]$.* Acta Arith. 22 (1973), 207-220.

[14] Y.-R. Yu, T. Wooley, *The unrestricted variant of Waring's problem in function fields.* Funct. Approx. Comment. Math. 37 (2007), 285-291.

E-mail address: `Arnaud.Bodin@math.univ-lille1.fr`

E-mail address: `Mireille.Car@univ-cezanne.fr`

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France

Université Paul Cézanne, Faculté de Saint-Jérôme, 13397 Marseille Cedex, France

[2] This is the bound used to fill the numerical table of the introduction.